

NOT FOR PUBLICATION

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

<p>ANNA V. ALONZO, on behalf of herself and others similarly situated,</p> <p style="text-align: center;">Plaintiffs,</p> <p style="text-align: center;">v.</p> <p>REFRESCO BEVERAGES US, INC.,</p> <p style="text-align: center;">Defendant.</p>	<p>Civil Action No. 23-22695 (GC) (JBD)</p> <p style="text-align: center;">MEMORANDUM OPINION</p>
---	--

CASTNER, District Judge

This matter comes before the Court upon Defendant’s Motion to Dismiss (ECF No. 20) the Complaint (ECF No. 1), pursuant to Federal Rule of Civil Procedure (Rule) 12(b)(1) and 12(b)(6). Plaintiff opposed and Defendant replied. (ECF Nos. 21 & 22.) The Court has carefully reviewed the parties’ submissions and decides the matter without oral argument pursuant to Rule 78(b) and Local Civil Rule 78.1(b). For the reasons set forth below, and other good cause shown, Defendant’s Motion is **GRANTED**.

I. BACKGROUND¹

A. Factual Background

Defendant Refresco Beverages US, Inc. is an independent beverage solutions provider that employs over 10,000 people across North America, Europe, and Australia. (ECF No. 1 ¶ 9.)

¹ On a motion to dismiss, the Court accepts as true all well-pled facts in the Complaint. *See Doe v. Princeton Univ.*, 30 F.4th 335, 340 (3d Cir. 2022) (quoting *Umland v. PLANCO Fin. Servs., Inc.*, 542 F.3d 59, 64 (3d Cir. 2008)).

Plaintiff Anna Alonzo and putative Class Members are Refresco employees and their spouses who entrusted Refresco with their personal identifiable information (“PII”). (*Id.* ¶ 10.) Refresco learned in May 2023 that it had suffered a “cybersecurity incident” affecting its North American network systems. In November 2023, Refresco notified its affected employees of this data breach via a letter (the “Notice Letter”). (*Id.* ¶¶ 11, 13.) Alonzo alleges that the nearly six-month delay between Refresco learning of the cybersecurity incident and its notification to employees prevented them from “taking important protective measures to ensure their PII was safe.” (*Id.* ¶¶ 13-14.)

In the Notice Letter, Refresco identified the following categories of information that were included in the data breach: social security numbers, financial account numbers, full names, home addresses, dates of birth, driver’s license numbers, health insurance policy numbers, and certain health information provided in connection with workers’ compensation and/or accommodations proceedings under the Americans with Disabilities Act. (*Id.* ¶ 15.) Alonzo claims that these categories of PII are “incredibly valuable” because they are “essential to conduct everyday business – from applying for employment or government benefits, to securing financing for major purchases such as a home or a vehicle.” (*Id.* ¶ 16.) Moreover, Alonzo alleges that she and the Class Members could become the victims of serious crimes, such as financial fraud and identity theft, if this information were to end up in the wrong hands. (*Id.*)

After providing notice of the data breach, Refresco offered its employees two years of free credit monitoring, which Alonzo counters is inadequate because “[d]ata thieves will be aware of the temporal scope of the protection offered . . . and can simply wait out the time as is the practice of such cyber criminals.” (*Id.* ¶ 26.) Alonzo further claims that such credit monitoring services do not prevent actual fraud—including draining bank accounts, stealing tax funds, and opening

utility accounts—so she and the Class Members will be forced to “employ heightened scrutiny to ensure that their PII is not being misappropriated.” (*Id.* ¶ 29.) As a result, Alonzo and the Class Members will “suffer far into the future, long after Refresco stops providing its employees credit monitoring or identity theft protection.” (*Id.*) Alonzo also claims that her information could find its way onto the “dark web” at an “undetermined point in the future.”² (*Id.* ¶ 28.)

B. Procedural Background

Alonzo filed this putative class action on November 28, 2023. Pursuant to Rule 23, Alonzo seeks to represent a class consisting of “[a]ll United States residents whose personal identifiable information was accessed without authorization in the data breach announced by Refresco in November of 2023.” (*Id.* ¶ 32.) Alonzo alleges that approximately 25,170 persons make up the class. (*Id.* ¶ 37.) Alonzo brings claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), and declaratory judgment (Count V). (*See generally id.*) Alonzo also brings a claim against Refresco under the New Jersey Consumer Fraud Act (Count IV) on behalf of a subclass of New Jersey residents “whose personal identifiable information was accessed without authorization in the data breach announced by Refresco.” (*Id.* ¶ 33.)

On March 1, 2024, Refresco moved to dismiss the Complaint pursuant to Rules 12(b)(1) and 12(b)(6). (ECF No. 20.) Alonzo opposed on March 18, and Refresco replied on March 25.

² Alonzo also appears to allege that she and the Class Members “suffered damages including . . . unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of PII of Plaintiff and Class Members,” and “damages arising from Plaintiff’s inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Breach and/or false or fraudulent charges stemming from the Breach.” (ECF No. 1 ¶¶ 66, 73.) As discussed herein, however, Alonzo claims to be pleadings these allegations “conjunctively and disjunctively” on behalf of the putative Class Members, (*see* ECF No. 21 at 15), and does not appear to allege that Alonzo herself suffered these injuries.

(ECF Nos. 21 & 22.)

II. LEGAL STANDARD

A. Rule 12(b)(1)

Rule 12(b)(1) permits a defendant to move at any time to dismiss the complaint for lack of subject-matter jurisdiction on either facial or factual grounds. *Gould Electronics Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000). A facial challenge asserts that “the complaint, on its face, does not allege sufficient grounds to establish subject matter jurisdiction.” *Iwanowa v. Ford Motor Co.*, 67 F. Supp. 2d 424, 438 (D.N.J. 1999). In analyzing a facial challenge, a court “must only consider the allegations of the complaint and documents attached thereto, in the light most favorable to the plaintiff.” *Gould Electronics Inc.*, 220 F.3d at 176. “A court considering a facial challenge construes the allegations in the complaint as true and determines whether subject matter jurisdiction exists.” *Arosa Solar Energy Sys., Inc. v. Solar*, Civ. No. 18-1340, 2021 WL 1196405, at *2 (D.N.J. Mar. 30, 2021).

A factual challenge, on the other hand, “attacks allegations underlying the assertion of jurisdiction in the complaint, and it allows the defendant to present competing facts.” *Hartig Drug Co. Inc. v. Senju Pharm. Co.*, 836 F.3d 261, 268 (3d Cir. 2016). The “trial court is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case” and “the plaintiff will have the burden of proof that jurisdiction does in fact exist.” *Petruska v. Gannon Univ.*, 462 F.3d 294, 302 n.3 (3d Cir. 2006) (quoting *Mortensen v. First Fed. Sav. & Loan Ass’n*, 549 F.2d 884, 891 (3d Cir. 1977)). “Therefore, a 12(b)(1) factual challenge strips the plaintiff of the protections and factual deference provided under 12(b)(6) review.” *Hartig Drug Co.*, 836 F.3d at 268. Regardless of the type of challenge, the plaintiff bears the “burden of proving that the court has subject matter jurisdiction.” *Cottrell v. Heritages Dairy Stores, Inc.*, Civ. No. 09-1743, 2010

WL 3908567, at *2 (D.N.J. Sep. 30, 2010) (citing *Mortensen*, 549 F.2d at 891).

B. Rule 12(b)(6)

On a motion to dismiss for failure to state a claim upon which relief can be granted, courts “accept the factual allegations in the complaint as true, draw all reasonable inferences in favor of the plaintiff, and assess whether the complaint and the exhibits attached to it ‘contain enough facts to state a claim to relief that is plausible on its face.’” *Wilson v. USI Ins. Serv. LLC*, 57 F.4th 131, 140 (3d Cir. 2023) (quoting *Watters v. Bd. of Sch. Directors of Scranton*, 975 F.3d 406, 412 (3d Cir. 2020)). “A claim is facially plausible ‘when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.’” *Clark v. Coupe*, 55 F.4th 167, 178 (3d Cir. 2022) (quoting *Mammana v. Fed. Bureau of Prisons*, 934 F.3d 368, 372 (3d Cir. 2019)). When assessing the factual allegations in a complaint, courts “disregard legal conclusions and recitals of the elements of a cause of action that are supported only by mere conclusory statements.” *Wilson*, 57 F.4th at 140 (citing *Oakwood Lab’ys LLC v. Thanoo*, 999 F.3d 892, 904 (3d Cir. 2021)). The defendant bringing a Rule 12(b)(6) motion bears the burden of “showing that a complaint fails to state a claim.” *In re Plavix Mktg., Sales Pracs. & Prod. Liab. Litig. (No. II)*, 974 F.3d 228, 231 (3d Cir. 2020) (citing *Davis v. Wells Fargo*, 824 F.3d 333, 349 (3d Cir. 2016)).

III. DISCUSSION

Refresco moves to dismiss on the basis that Alonzo does not have Article III standing.³ Because the Court finds that Alonzo has not alleged an imminent injury for purposes of standing, the Court will dismiss the Complaint.

³ The Court understands Refresco to be making a facial attack on standing, and the parties appear to concede that this is a facial attack. (See ECF No. 21 at 17; see generally ECF No. 22.) While Refresco appears to dispute certain allegations in the Complaint, it is apparent that Refresco

A. Article III Standing

Deriving from the Constitution’s limit on the judicial power to resolve “actual cases and controversies,” standing “is the threshold question in every case and determines the power of the court to entertain the suit.” *Bittner v. Waterford Twp. Sch. Dist.*, Civ. No. 18-10990, 2020 WL 10223599, at *2 n.2 (D.N.J. Jan. 13, 2020) (quoting *Warth v. Seldin*, 422 U.S. 490, 498 (1975)). “Standing is a question of subject matter jurisdiction.” *Petroleos Mexicanos Refinacion v. M/T KING, A (Ex-Tbilisi)*, 377 F.3d 329, 224 (3d Cir. 2004). “Absent Article III standing, a federal court does not have subject matter jurisdiction to address a plaintiff’s claims.” *Taliaferro v. Darby Twp. Zoning Bd.*, 458 F.3d 181, 188 (3d Cir. 2006). Article III standing requires a plaintiff to demonstrate “(1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief.” *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 152 (3d Cir. 2022) (quoting *Thole v. U. S. Bank N.A.*, 590 U.S. 538, 540 (2020)). However, “where the future injury is also hypothetical, there can be no imminence and therefore no injury-in-fact.” *Id.* at 153. “A harm is ‘actual or imminent’ rather than ‘conjectural or hypothetical’ where it is presently or actually occurring, or is sufficiently imminent. . . . [P]laintiffs relying on claims of imminent harm must demonstrate that they face a realistic danger of sustaining a direct injury from the conduct of which they complain.” *Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 278 (3d Cir. 2014). “An allegation of future injury may suffice if the threatened injury is certainly

is arguing that certain allegations are not well-pled and therefore should not be accepted as true for purposes of establishing subject-matter jurisdiction. (See ECF No. 22 at 6 (“Refresco’s actual assertion is that the allegations in the Complaint are not properly pled.”).) Thus, the Court will “consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff.” *Lincoln Ben. Life Co. v. AEI Life, LLC*, 800 F.3d 99, 105 (3d Cir. 2015).

impending, or there is a substantial risk that the harm will occur.” *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted).

Refresco argues that “Plaintiff fails to allege [a] concrete injury sufficient to establish standing,” (ECF No. 20-2 at 5⁴), which the Court construes as an attack on whether Alonzo has alleged an imminent injury-in-fact or a substantial risk that a harm will occur. As explained below, the Court agrees that Alonzo lacks standing for failing to satisfy the injury-in-fact requirement.

1. Standing for Data Breach Plaintiffs

The United States Court of Appeals for the Third Circuit has previously analyzed whether data breach plaintiffs, like Alonzo, can satisfy the “actual or imminent” injury requirement to have standing in federal court. *See Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022) (finding the plaintiffs had standing); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (finding the plaintiffs did not have standing).

In *Reilly*, a payroll processing company, Ceridian, was infiltrated by an unknown hacker. 664 F.3d at 40. While the hacker “potentially gained access to personal and financial information belonging to [the plaintiffs] and approximately 27,000 employees at 1,900 companies,” it was “not known whether the hacker read, copied, or understood the data.” *Id.* After working with law enforcement and professional investigators, Ceridian notified potentially impacted individuals that their personal information, including their “first name, last name, social security number and, in several cases, birth date and/or the bank account that is used for direct deposit” had potentially been “illegally accessed by an unauthorized hacker.” *Id.* The plaintiffs—employees of a law firm that used Ceridian to process its payroll—alleged that they “ha[d] an increased risk of identity

⁴ Page numbers for record cites (*i.e.*, “ECF Nos.”) refer to the page numbers stamped by the Court’s e-filing system and not the internal pagination of the parties.

theft, (2) incurred costs to monitor their credit activity, and (3) suffered from emotional distress.”
Id.

In finding that the plaintiffs lacked standing, the Third Circuit reasoned that “allegations of hypothetical, future injury do not establish standing under Article III.” *Id.* at 41. The Court explained that “[the plaintiffs] have alleged no misuse, and therefore, no injury. Indeed, no identifiable taking occurred; all that is known is that a firewall was penetrated. [The plaintiffs’] string of hypothetical injuries do not meet the requirement of an ‘actual or imminent’ injury.” *Id.* at 44. The Court also held that money spent by the plaintiffs protecting against a potential injury was insufficient to confer standing because they had not alleged an actual injury. *Id.* at 46 (“Although [the plaintiffs] have incurred expenses to monitor their accounts and ‘to protect their personal and financial information from imminent misuse and/or identity theft,’ they have not done so as a result of any actual injury (e.g. because their private information was misused or their identities stolen). Rather, they prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent.” (internal citations omitted)).

Clemens, on the other hand, involved an injury that the Third Circuit described as “far more imminent” than the one alleged in *Reilly*. 48 F.4th at 156. There, a sophisticated hacker group known as “CLOP” accessed the plaintiff’s sensitive data and placed it on the “dark web.” *Id.* at 156-57. In her complaint, the plaintiff characterized the dark web as being “most widely used as an underground black market where individuals sell illegal products like drugs, weapons, counterfeit money, and sensitive stolen data that can be used to commit identity theft or fraud.” *Id.* at 157.

The Court, adopting a set of non-exhaustive factors used in other circuits, analyzed (1) whether the breach was intentional, (2) whether the data was misused, and (3) the nature of the

information accessed through the breach. *Id.* at 153-54. No one factor is dispositive. *Id.* at 153. Applying these factors, the Court concluded that the plaintiff had alleged a sufficient injury for purposes of Article III standing, namely that her risk of identity theft or fraud was “sufficiently imminent.” *Id.* at 159. It reasoned that “CLOP intentionally gained access to and misused the data: it launched a sophisticated phishing attack to install malware, encrypted the data, held it for ransom, and published it.” *Id.* at 157. The Court also noted that the combination of both personal and financial information included in the leak was particularly concerning. *Id.*

With respect to the “misuse” prong, the Court found that due to the nature of the dark web and those who use it, the plaintiff’s allegation that her data was published on the dark web was significant in showing that she faced a substantial risk of identity fraud. *Id.* The Court explained:

Because we can reasonably assume that many of those who visit the Dark Web, and especially those who seek out and access CLOP’s posts, do so with nefarious intent, it follows that [the plaintiff] faces a substantial risk of identity theft or fraud by virtue of her personal information being made available on underground websites.

[*Id.*]

As the Third Circuit made clear, *Clemens* did not overrule *Reilly*, but rather addressed a factually distinguishable situation that dictated a different result. *See Clemens*, 48 F.4th at 159. While the Third Circuit expressly rejected a “bright line” rule which would preclude standing for “allegations of an increased risk of identity theft resulting from a security breach,” it reaffirmed that courts must determine “whether an injury is present versus future, and imminent versus hypothetical.” *Id.* at 153. Accordingly, a *future* injury that is also *hypothetical* is insufficient for purposes of establishing standing. *See id.*; *see also In re Am. Fin. Res., Inc. Data Breach Litig.*, Civ. No. 22-01757, 2023 WL 3963804, at *5 (D.N.J. Mar. 29, 2023) (finding that a plaintiff who did not allege that his “PII was accessed and disseminated” had “not established actual or imminent

injury sufficient to confer standing”).

2. *Clemens Factors*

The Court analyzes Alonzo’s claims using the three-factor test used by the Third Circuit in *Clemens*.

a. *Whether the breach was intentional*

The first factor is whether the breach was intentional. An intentional breach makes standing more likely. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 301 (2d Cir. 2021). Here, Alonzo alleges that Refresco—in an attempt to downplay the seriousness of the breach—characterized the breach as a “cyber incident.” (ECF No. 1 ¶ 18.) She further alleges that Refresco has done nothing to “protect 25,170 employees who had their PII exposed to criminals.” (*Id.* ¶ 27.) As another court in this Circuit has observed, “all cyber-attacks involve some degree of intentional conduct just by the very nature of the attack.” *McGowan v. CORE Cashless, LLC*, Civ. No. 23-00524, 2023 WL 8600561, at *9 (W.D. Pa. Oct. 17, 2023), *report and recommendation adopted*, Civ. No. 23-00524, 2024 WL 488318 (W.D. Pa. Feb. 8, 2024). With that in mind, however, the Court finds that this case involves a level of intentionality more akin to *Reilly* than to *Clemens*.

Unlike *Clemens*, which involved CLOP, a “sophisticated ransomware group,” accessing the plaintiff’s data, 48 F.4th at 157, Alonzo does not set forth any specific allegations about who was behind the Refresco data breach. (*See* ECF No. 1 ¶ 49 (referring to the alleged hacker as an “unknown third party”).) Moreover, Alonzo does not allege that the hacker actually accessed her specific data. To the contrary, Alonzo alleges that because of the data breach, she and the class members will have to “expend time and resources *investigating the extent to which their PII has been compromised.*” (ECF No. 1 ¶ 75 (emphasis added).) The allegations are therefore similar to

Reilly, where “an unknown hacker infiltrated [the company’s] system and potentially gained access to personal and financial information belonging to” the plaintiffs. 664 F.3d at 40. Courts have found that data breach plaintiffs lacked standing under similar circumstances. *See In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *5 (finding that a plaintiff alleging a “criminal” hack by unknown individuals that could not “meaningfully allege that the information accessed in the breach was mass-published onto the dark web, or otherwise disseminated” lacked standing); *In re Retreat Behav. Health LLC*, Civ. No. 23-00026, 2024 WL 1016368, at *3 (E.D. Pa. Mar. 7, 2024) (finding plaintiff who alleged that an “unknown hacker . . . potentially gained access to sensitive information” did not have standing (quoting *Clemens*, 48 F. 4th at 156)). Based on the relatively sparse nature of the allegations concerning the intention behind the data breach, the Court finds that this factor weighs in favor of a finding that Alonzo lacks standing.

b. Whether the data was misused

Next, the Court must consider whether Alonzo’s data was actually misused. In *Clemens*, the Third Circuit clarified its holding in *Reilly* and made clear that misuse of data is not necessarily required for a plaintiff to have standing. *Clemens*, 48 F. 4th at 154. But here, Alonzo does not allege misuse or any facts that point to imminent misuse or even a risk of future harm. *Cf. id.* at 157 (finding that where the plaintiffs’ sensitive information was published on the dark web, their alleged injuries were sufficiently imminent because of the nefarious nature of the dark web and those who frequent it). Unlike in *Clemens*, there are no allegations that Alonzo’s PII was published on the dark web. To the contrary, Alonzo alleges a number of hypotheticals, like that her “PII may also be sold on the ‘dark web’ at *some undetermined point in the future.*” (ECF No. 1 ¶ 28 (emphasis added).) The circumstances here are more akin to *Reilly*, which “depended upon a string of hypotheticals being borne out.” *Id.*

Alonzo argues that Refresco inaccurately frames *Clemens* as a “dark web litmus test” under which “if the information was published on the ‘dark web’ then there is standing and if not then there is no standing.” (ECF No. 21 at 22.) The Court does not read *Clemens* to establish or endorse such a litmus test. Publication on the dark web is not a prerequisite for standing in the data breach context, but it is simply one of several facts that a plaintiff can point to in order to establish that their data was misused and an injury is imminent. *See, e.g., In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, Civ. No. 19-02904, 2021 WL 5937742, at *8 (D.N.J. Dec. 16, 2021) (“The fraudulent charges identified by the [plaintiffs] permit the inference that their specific information has been accessed and misused.”).

Alternatively, Alonzo argues that Refresco’s arguments regarding “misuse” have “lost favor” in the Third Circuit but she has nevertheless alleged misuse in her Complaint. (ECF No. 21 at 18-21.) Taking those in order, the Third Circuit made clear in *Clemens* that misuse is just one of the “useful guideposts” to consider in determining whether a data breach plaintiff has standing. 48 F.4th at 153. In terms of the misuse of her own data, Alonzo cites to several allegations in her Complaint to support her contention that she properly pled that her data has been misused. (ECF No. 21 at 20.) For instance, she alleges that “Refresco failed to provide adequate supervision and oversight of the PII which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.” (ECF No. 1 ¶ 49.) She also alleges that “Refresco’s breach of its duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiff and the Class Members without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and other unauthorized access.” (ECF No. 1 ¶ 74.)

Courts, however, have found similar allegations insufficient to establish that a plaintiff's data was misused. *See Reilly*, 664 F.3d 38; *Boje v. Mercyhurst Univ.*, Civ. No. 23-00046, 2024 WL 964892, at *4 (W.D. Pa. Mar. 6, 2024) (finding that the plaintiff “failed to plausibly show that his threatened risk of harm from the Data Breach [was] imminent” in part because “[u]nlike in *Clemens*, there is no allegation that the information compromised by the Data Breach in the present case was ever published on the Dark Web or otherwise distributed or made available to ‘nefarious’ third parties.”); *In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804, at *5 (finding that the plaintiff’s general allegations that “‘criminals’ hacked into [defendant’s] systems with the intent to misuse PII” did not establish imminent injury to confer standing because the plaintiff could not “meaningfully allege that the information accessed in the breach was mass-published onto the dark web, or otherwise disseminated”); *cf. Adkins*, 2024 WL 3887127, at *5 (finding that a plaintiff who alleged her name and social security number were accessed in a data breach and that an unauthorized party attempted to access her checking account satisfied the standing requirement “by a thin reed”).

Moreover, Alonzo’s allegations are significantly different from the allegations that the Third Circuit in *Clemens* cited as examples of misuse. *See, e.g., Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010) (finding there was standing where a laptop with personal unencrypted data was stolen and a plaintiff further alleged that someone “attempted to open a bank account in his name”); *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 692-94 (7th Cir. 2015) (finding there was standing where the plaintiff alleged that personal data had “already been stolen” and that 9,200 people had “incurred fraudulent charges”). Unlike the specific allegations of misuse in other cases, Alonzo’s allegations concerning misuse are conclusory or merely hypothetical, and therefore insufficient to establish standing. (*See, e.g.,* ECF No. 1 ¶ 74 (“Refresco’s breach of its

duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiff and the Class Members without authorization.”)); *In re Asbestos Prod. Liab. Litig. (No. VI)*, 822 F.3d 125, 133 (3d Cir. 2016) (“[D]istrict courts are not required to accept merely conclusory factual allegations or legal assertions.”). Thus, the Court finds this factor weighs in favor of a finding that Alonzo has not alleged an injury-in-fact. Alonzo has not sufficiently alleged that her data was misused and an injury is imminent.

c. The nature of the information accessed

Finally, the type of information implicated in a data breach may affect whether a plaintiff has standing. *Clemens*, 48 F.4th at 154. In particular, the “disclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud.” *Id.* But even in cases involving disclosure of highly sensitive information, standing is not automatic. *See McMorris*, 995 F.3d at 304 (“[W]hile the information that was inadvertently disclosed by CLA included the sort of PII that might put [p]laintiffs at a substantial risk of identity theft or fraud, in the absence of any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused, this factor alone does not establish an injury in fact.”).

Here, Alonzo alleges that the type of information involved in the Refresco data breach—home addresses, email addresses, dates of birth, social security numbers, financial account numbers, health insurance policy numbers, and other health information (ECF No. 1 ¶ 15)—is more akin to the data at issue in *Clemens*. (ECF No. 21 at 21-22); *see Clemens*, 48 F.4th at 150 (stolen information included “social security numbers, dates of birth, full names, home addresses, taxpayer identification numbers, banking information, credit card numbers, driver’s license numbers, sensitive tax forms, and passport numbers”). The Court finds that, due to the sensitive nature of the potentially impacted data, particularly social security numbers, names, and dates of

birth, this factor cuts in favor of a finding that Alonzo has alleged an injury-in-fact. *See Clemens*, 48 F.4th at 157 (finding that the “combination of financial and personal information is particularly concerning as it could be used to perpetrate both identity theft and fraud.”)

Having considered the factors set forth above, the Court concludes that Alonzo has not met her burden of establishing that she has standing for subject-matter jurisdiction. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992) (the elements of standing “are not mere pleading requirements but rather an indispensable part of the plaintiff’s case,” and “each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof”).

On balance, Alonzo’s allegations are more consistent with those in *Reilly* than in *Clemens*. Even accepting all of her well-pled allegations as true, Alonzo has only pled that she will suffer *future* injuries, which is not necessarily fatal to her claim but requires her to plead that her “injury is certainly impending, or there is a substantial risk that the harm will occur.” *See Susan B. Anthony List*, 573 U.S. at 158 (internal quotation marks omitted); *Rauhala v. Greater New York Mut. Ins., Inc.*, Civ. No. 22-1788, 2022 WL 16553382, at *3 (E.D. Pa. Oct. 31, 2022) (“Although an injury that will occur in the future is not fatal to standing, the risk of injury cannot be hypothetical or speculative” (citing *Clemens*, 48 F.4th at 153)).

Although at the motion to dismiss stage the Court must accept a plaintiff’s well-pled allegations as true, the bulk of Alonzo’s alleged injuries are hypothetical and concern only the possibility that she may suffer adverse consequences in the future. (*See, e.g.*, ECF No. 1 ¶¶ 28-29 (alleging that drained bank accounts and stolen tax refunds are among the “harms that Plaintiffs and Class Members can suffer *far into the future*,” and that the “stolen PII *may* also be sold on the ‘dark web’ *at some undetermined point in the future*”) (emphasis added).) She also alleges that “[d]ata thieves . . . can simply wait out the time as is the practice of such cyber criminals.” (*Id.* ¶

26.) Taken together, Alonzo’s allegations simply do not satisfy her burden of showing an “actual or imminent” injury because she has not connected her forward-looking claims to an imminent injury. Courts in this circuit have routinely rejected claims that are factually analogous to those brought here. *See, e.g., Reilly*, 664 F.3d 38; *In re Retreat Behav. Health LLC*, 2024 WL 1016368; *In re Am. Fin. Res., Inc. Data Breach Litig.*, 2023 WL 3963804; *McGowan*, 2023 WL 8600561.

In paragraphs 66 and 73 of the Complaint, Alonzo alleges what could be characterized as “actual” harms, including that “Plaintiff and the Class suffered . . . unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of PII of Plaintiff and Class Members,” and “damages arising from Plaintiff[s]’ inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Breach.” (ECF No. 1 ¶¶ 66, 73.) In its Motion, Refresco suggests that these paragraphs “may have been included as a drafting error” because “such fraud would necessarily be supported by documents and no such documents were appended to or referenced in the Complaint.” (ECF No. 20-2 at 8.) In support, Refresco points to near-verbatim language in a complaint filed in an unrelated case, *Hameed-Bolden v. Forever 21 Retail, Inc.*, Civ. No 18-03019 (C.D. Cal.) (alleging “Plaintiffs and Class members suffered . . . unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Customer Data of Plaintiffs and Class members” and “damages arising from Plaintiffs’ inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach”). (ECF No. 20-2 at 7-8.)

Refresco also points out that (1) allegations of credit card numbers being leaked appear nowhere else in the Complaint, and (2) the Notice Letter makes no mention of leaked credit or

debit card information.⁵ (*Id.*)

According to Alonzo, the claims regarding credit card fraud were being pled “conjunctively and disjunctively.” (ECF No. 21 at 15.) In her opposition brief, Alonzo suggests that this “conjunctive and disjunctive” pleading is appropriate because she herself has “suffered at least one concrete measure of damages as a result of the substantial risk, i.e. lost time to mitigate and monitor found to be ‘concrete.’” (*Id.* at 15, 24.) In other words, Alonzo appears to concede that she has not actually suffered these concrete harms as alleged.

The Court will not consider these factual allegations for purposes of analyzing standing. A named plaintiff cannot rely on the potential claims of unnamed class members to satisfy the Article III standing requirement. *See Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 n.6 (2016), *as revised* (May 24, 2016) (“That a suit may be a class action . . . adds nothing to the question of standing, for even named plaintiffs who represent a class ‘must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong.’” (quoting *Simon v. Eastern Ky. Welfare Rights Organization*, 426 U.S. 26, 40, n. 20 (1976))). This is equally true in the data breach context. *See In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *10 (holding that because “others have suffered some concrete injury following” a data breach was “insufficient to establish the particularized reasonableness” of the plaintiffs’ “fears of future harm”).

In addition, the Court concludes that the allegations in paragraphs 66 and 73 of Alonzo’s

⁵ The Court may properly consider the Notice Letter at the motion to dismiss stage because it is specifically referenced in Alonzo’s Complaint and attached to Defendant’s motion, and Alonzo does not dispute the document’s authenticity. *See Pension Ben. Guar. Corp. v. White Consol. Indus., Inc.*, 998 F.2d 1192, 1196 (3d Cir. 1993) (“[A] court may consider an undisputedly authentic document that a defendant attaches as an exhibit to a motion to dismiss if the plaintiff’s claims are based on the document.”).

Complaint are not well-pled based on the Notice Letter, which makes no reference to any leaked credit or debit card information. The Court does not have to accept these allegations as true. *See Nasyrova v. Immunomedics, Inc.*, Civ. No. 14-1269, 2015 WL 4388310, at *3 (D.N.J. July 15, 2015) (finding that the requirement to accept all allegations as true “does not apply when the allegations are contradicted by the documents attached to the Complaint upon which its claims are based”). Based on the allegations as currently pled, Alonzo has not satisfied her burden to show that she has Article III standing. *See Lujan*, 504 U.S. at 555 (holding that plaintiffs “bear the burden of showing standing”).

Besides relying on *Clemens* itself, Alonzo also argues the allegations are similar to those in *Rauhala*, 2022 WL 16553382, where the court found standing. (ECF No. 21 at 22-23.) In that case, like here, the plaintiff brought a putative class action following a cyberattack and data breach. *Rauhala*, 2022 WL 16553382, at *1. The plaintiff in *Rauhala*, however, alleged several injuries, including the sale of her information on the dark web, an increase in spam calls, and actual identity theft. *Id.* While the plaintiff there also pointed to some imminent injuries, the court’s ultimate ruling rested on the fact that the plaintiff had alleged “actual, tangible injuries from the data breach,” not mere hypothetical or future injuries. *See id.* at *3; *see also Salas v. Acuity-CHS, LLC*, Civ. No. 22-00317, 2023 WL 2710180, at *4 (D. Del. Mar. 30, 2023) (finding that the plaintiff alleged a “sufficiently imminent” future injury where she claimed that her information was “for sale to criminals on the dark web” and that she “received an alert through her identity theft monitoring service that her email address had recently been used in a potential identity theft incident”).

Since the Court finds that Alonzo’s claims involve future harms that are merely hypothetical, the Court must dismiss Alonzo’s Complaint for lack of subject-matter jurisdiction.

At bottom, Alonzo's claims rely on the same speculative chain of events that the Third Circuit rejected in *Reilly*: "if the hacker read, copied, and understood the hacked information, and if the hacker attempts to use the information, and if he does so successfully, only then will [plaintiff] have suffered an injury." *Reilly*, 664 F.3d at 43.

B. Failure to State a Claim

Finding that Alonzo lacks standing to bring her Complaint, the Court does not address whether she has stated a claim for relief. *See Cottrell v. Alcon Lab's*, 874 F.3d 154, 164 n.7 (3d Cir. 2017) ("[T]he absence of standing leaves the court without subject matter jurisdiction to reach a decision on the merits."); *In re Retreat Behav. Health LLC*, 2024 WL 1016368, at *1 n.1 ("The [c]ourt need not address the merits in this matter because it lacks jurisdiction.").

IV. CONCLUSION

For the reasons set forth above, Defendant's Motion to Dismiss (ECF No. 20) is **GRANTED**. Plaintiff's Complaint is **DISMISSED** without prejudice. To the extent that Plaintiff can cure the deficiencies in her Complaint, Plaintiff will be given leave to amend within thirty (30) days. An appropriate Order follows.

Dated: September 30, 2024


 GEORGETTE CASTNER
 UNITED STATES DISTRICT JUDGE